

REDITE.

Cyber & Data Security

Reseller Sales & Support Guide



AUTHORISED
RESELLER



TABLE OF CONTENTS

Item	Page Number
About Sentry Bay & Redite	3
Evolution of Sentry Bay	4
Redite Global Footprint	5
Usage Cases	6
Current Endpoint Issues	7
Current Risks	8
The Armored Client Solution	9
Tier 1 Protection	10
Tier 2 Protection	11
Protection and Overview of Armored Client	12
Armored Client Containerization	13
Administration Portal Overview	14 – 15
Armored Client Benefits	16
Product Features and Comparison	17 – 19
Overview & Options of Armored Client	20
Retail Pricing and Rates Card	21
Computer Troubleshooters Net Revenue Share	22
Computer Troubleshooters Customer Process	23
Service and Support Overview	24
Sales & Support Contact Details / Procedures	25
Sales Collateral Overview	26

Exclusive Authorised Distributor

ABOUT SENTRY BAY



SentryBay have been pioneers in developing technology that approaches security issues from a different, more proactive perspective.

Focusing on Endpoint data protection, as this is essential to provide a secure cloud-based IT ecosystem that avoids the weaknesses inherent in both technology and users.

REDITE IS THE EXCLUSIVELY AUTHORISED DISTRIBUTOR OF SENTRYBAY IN BOTH ASIA PACIFIC AND AFRICA.

SentryBay is a Private Company and was founded in 2002.

SentryBay's headquarters is based in London, United Kingdom.

Redite has sales offices located in Melbourne, USA & South Africa.

Current patents have been granted to three of our key technologies.

SentryBay has helped over 5 million Users.

EVOLUTION OF



Version 1 of the 'Armored Client for Citrix' developed which overlays the users screen

2015



The 'Armored Client' is launched to target all Remote Access, Internal Enterprise and External SaaS Apps

2019



REDITE.
Cyber & Data Security

2011

Armored Browser is released by SentryBay



2018

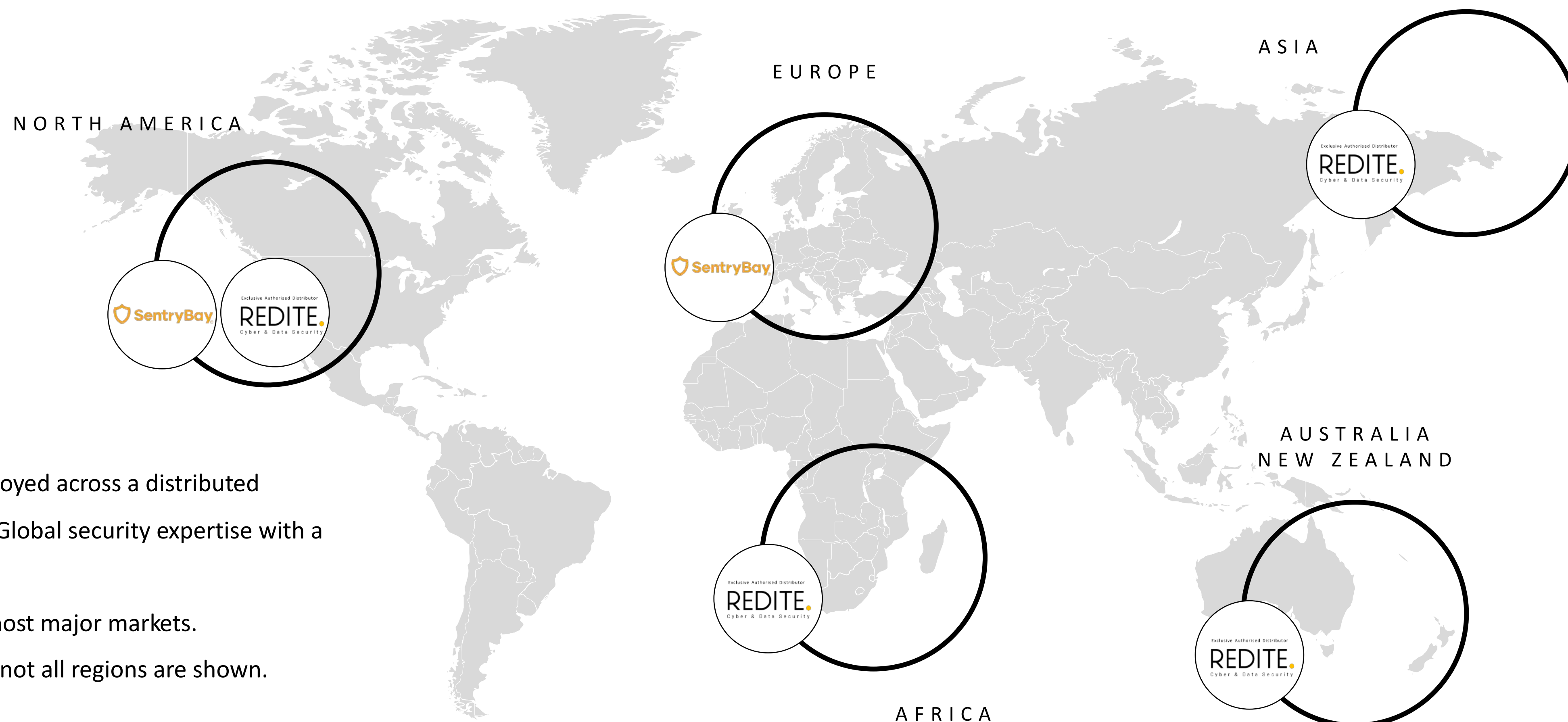
The 'Armored Client for Citrix' is updated, providing a more seamless user experience



2020

Additional features including Credential Monitoring, Advanced Malware Detection and Mobile clients to be included into the 'Armored Client'

THE REDITE FOOTPRINT



Security that can be deployed across a distributed international operation. Global security expertise with a local hands-on feel.

With representation in most major markets.

Map for illustration only, not all regions are shown.

TRUSTED BY BIG COMPANIES

CUSTOMERS: ENTERPRISE



CUSTOMER: OEM SOLUTIONS



Customer: Consumer ID Theft Protection Products



CURRENT ENDPOINT ISSUES

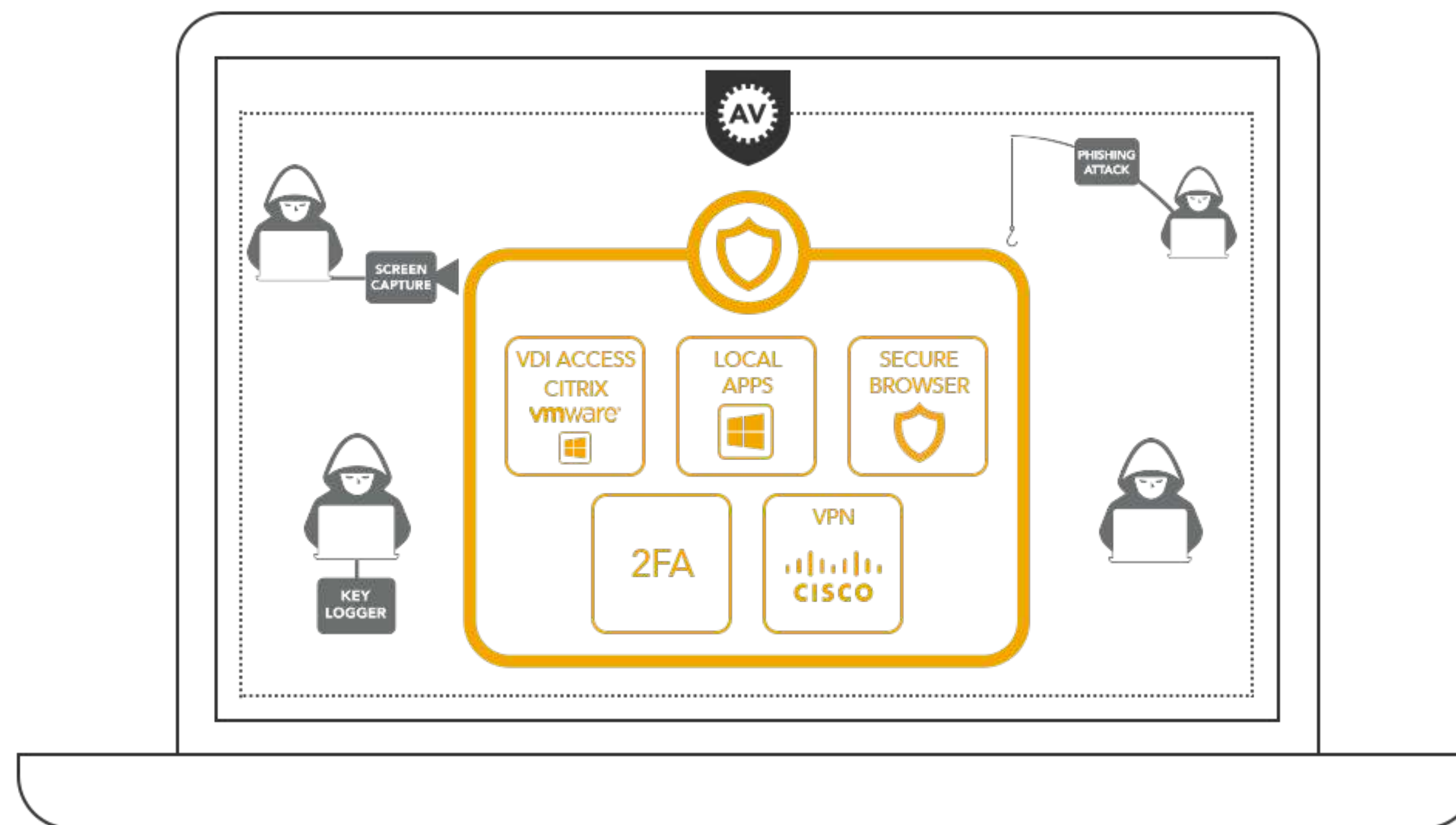
**70% of breaches
originating at
the endpoint**

Absolute 2019 Global Endpoint
Security Trend Report

**42% of all endpoints
are unprotected
at any given time**

Absolute 2019 Global Endpoint
Security Trend Report

**230,000 new malware
samples created every day**



**Number one ranked
global
malware is spyware /
keyloggers**

NTT Security Threat Intelligence Report 2018
<https://attack.mitre.org/techniques/T1056>

**Average breach takes
minutes to take effect
and over 200 days to
be discovered**

Verizon 2016 Data Breach Investigation Report

CURRENT RISKS

Organisations are using remote access / web based solutions to enable the workforce to be more flexible and in return, productivity has increased. The endpoint is regarded as the largest risk, especially on unmanaged devices, so what are those risks?

<div>➤</div> GENERAL RISKS	<div>➤</div> SPECIFIC THREATS FOR REMOTE ACCESS / WEB APPS
<ul style="list-style-type: none"> Elevated User Privileges Phishing Attacks Relaxed Device Security Posture Shared Devices Counterfeit or Malicious Software Untrusted Wireless Networks 	<ul style="list-style-type: none"> Keylogging Screen Capture / Scraping Browser Attacks (MiM, MiB, DLL Injection) RDP Double-Hop VNC Attacks – Screen Mirroring Saved Account Detail Harvesting

THE SOLUTION COMPONENTS

Data Security and compliance within an enterprise is ever-changing to mitigate risk and adhere to best practices the Armored client meets a range of compliance requirements.



ARMORED CLIENT

SentryBay Armored Client provides real time patented protection to applications & data without needing to detect & respond to threats, kernel level prevention of data exfiltration even if the threats exist. Combined with the secure wrapping of applications and injected security. Including an independent customisable secure Armored Client Browser.

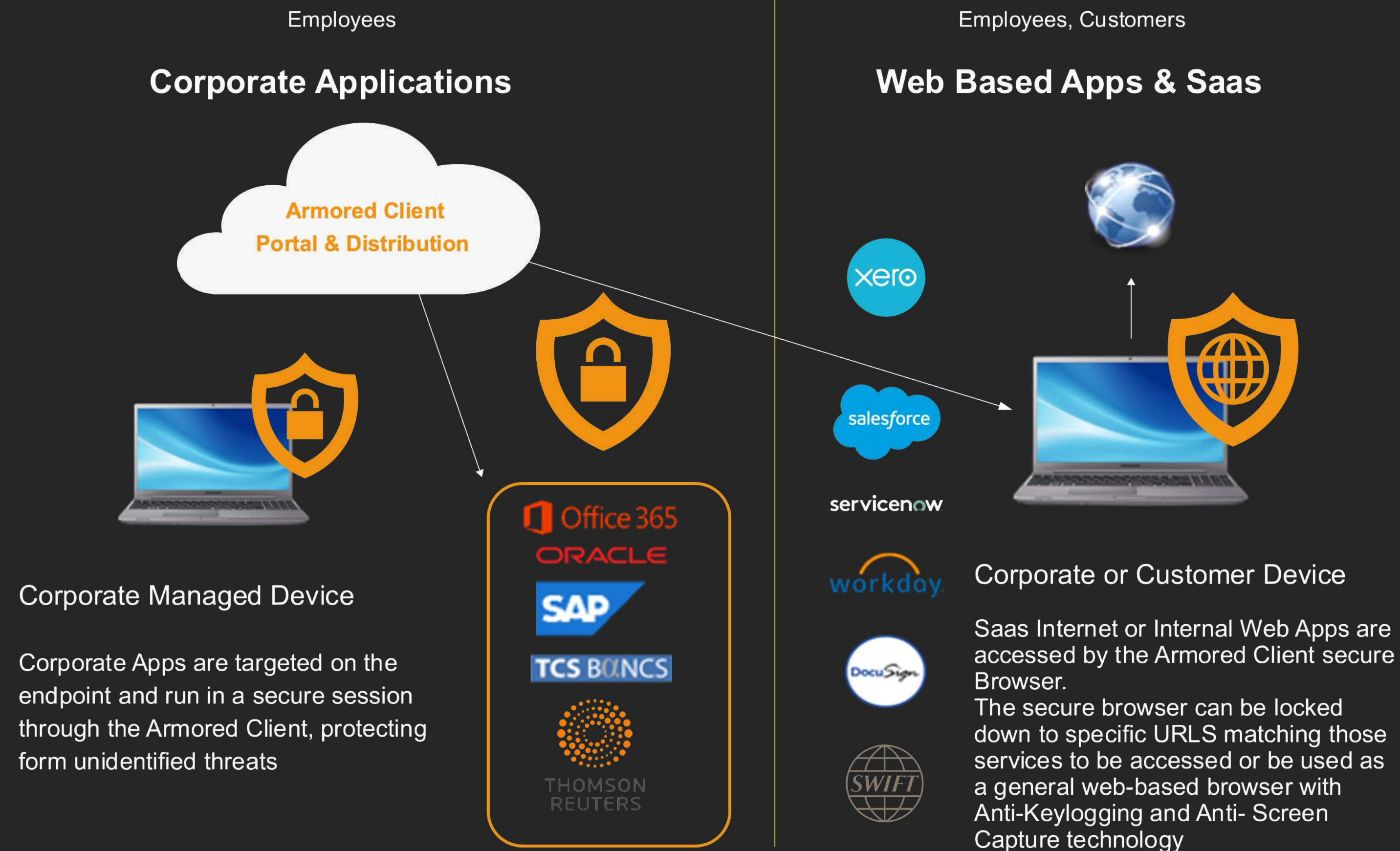


ARMORED BROWSER

The Armored Browser is the premier browser-based solution designed for secure access to any SaaS application. It is ideal for protecting online banking, brokerage, wealth management, insurance, healthcare, government and e-commerce portals. It creates a secure environment in order to maximise security – without compromising usability. The product also includes SentryBay's patented EntryProtect anti-keylogging technology.

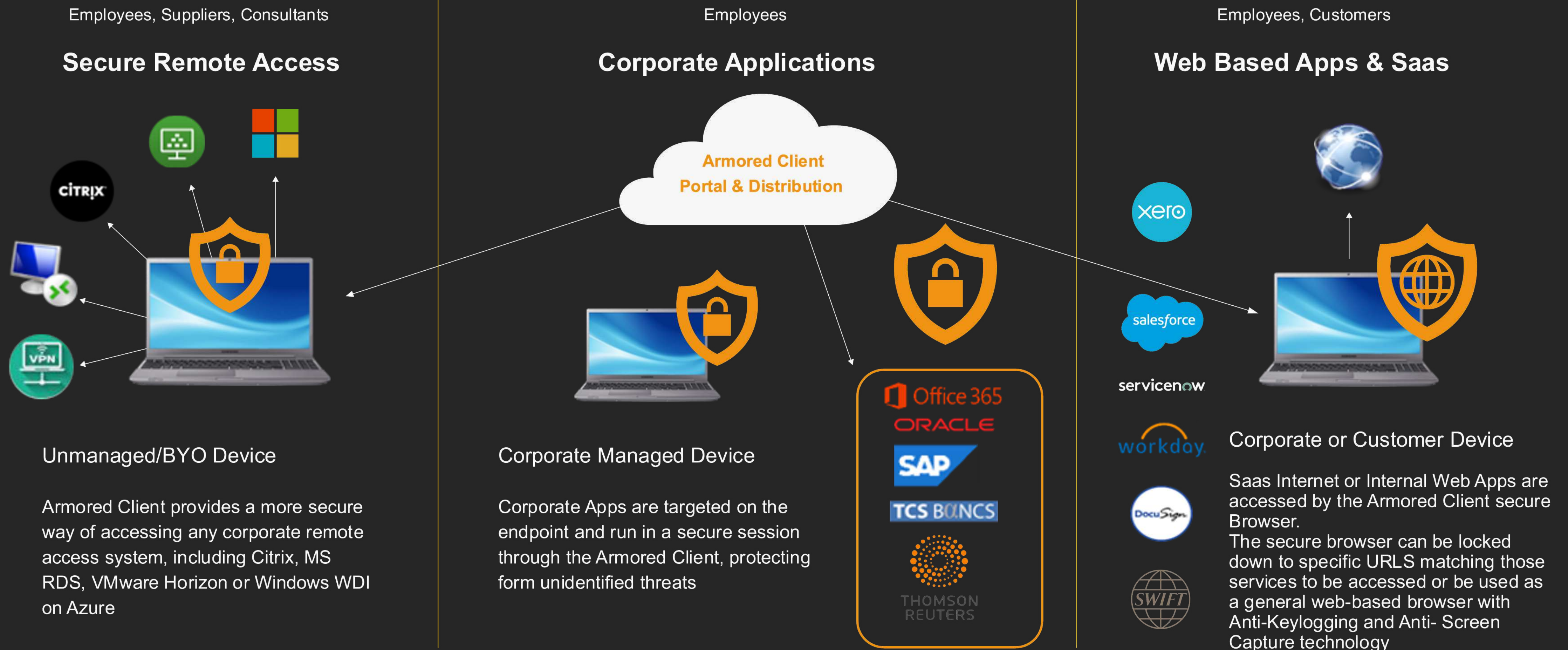
WHAT DOES THE TIER 1 ARMORED CLIENT PACKAGE PROTECT?

10



WHAT DOES THE TIER 2 ARMORED CLIENT PACKAGE PROTECT?

11



USER ARMORED CLIENT



Entry Protect & Secure Framework

provide Data security layers to nominated PC-based application-
i.e.. Microsoft Word, Excel, Outlook, PowerPoint, Publisher,
OneNote



Remote Access solutions

Such as Citrix, VMware Horizon, Windows Virtual Desktop, Amazon
Workspaces or legacy RDS environments.



Configurable Secure Browser

Based on Chromium Code, with patented SentryBay Core Security
Features embedded to secure Data



Kernel level Anti Keylogging

Protecting data as it is being created when users are typing



Anti Screen Capture

Protecting data from Screen capture malware



MITM / MITB Attacks

Via the use of the Armored Browser

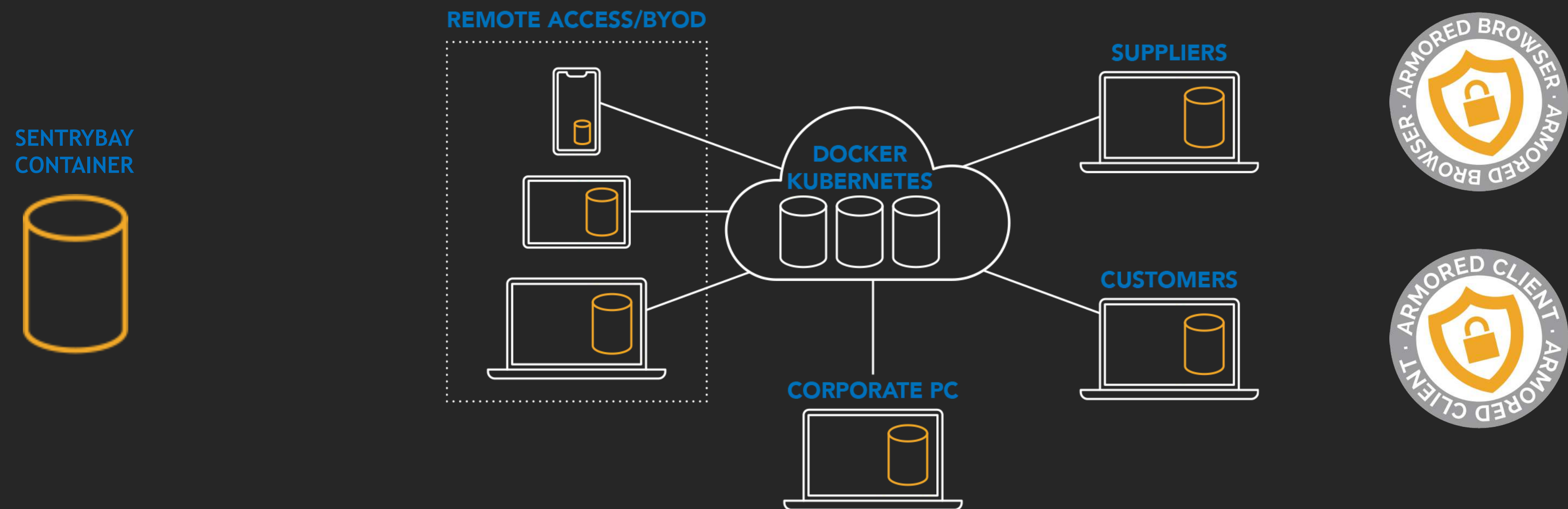


RDP Double Hop Protection

ARMORED CLIENT PROTECTS AGAINST:

- ❖ Keylogging (incl. kernel level)
- ❖ Screen Capture
- ❖ RDP Double-hop
- ❖ DLL/Code hooking Injection
- ❖ Code execution protection
- ❖ DNS attack
- ❖ MiTM - Man-in-the-middle attack
- ❖ MiTB - Man-in-the-browser
- ❖ And more...



HOW OUR SOLUTION CAN BE APPLIED TO YOUR ENVIRONMENT TO SECURE YOUR COMPANY DATA



- SentryBay operates on endpoints securing strategic vulnerabilities in the cloud ecosystem
- Armored Client securely wraps nominated Programs, remote access, enterprise and SaaS apps
- Combination of simple containerisation/injected security/kernel level anti-key logging
- Provides real time patented protection to applications & data without needing to detect & respond to threats

ARMORED CLIENT ADMIN PORTAL

14



MENU


Dashboard

Home


Companies

Admins


Description




Installed Browsers
Chrome, Firefox, Internet Explorer, Edge, Safari




Microsoft 365
Microsoft Word, Excel, Outlook, PowerPoint




Secure Browser
Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking




Remote Access
Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces.



Whitelisted Collaborative Software
TeamViewer, GoToMeeting, RealVNC, Microsoft Teams, Zoom.



Registry
Add, Sync and Delete Registry Keys





Custom Settings
Block RDP, Block VM, Protect Clipboard.

Installed Browsers

Chrome, Firefox, Internet Explorer, Edge, Safari



Chrome

☐




Firefox

☐





Internet Explorer

☐




Edge

☐



Safari

☐



Microsoft Office

Microsoft Word, Excel, Outlook, PowerPoint

Microsoft Word

☐

Microsoft Excel

☒

Microsoft Outlook

☐

Microsoft PowerPoint


☐

Cancel


Save

Remote Access


Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces.

 Citrix


☐

 VMware Horizon


☐

 Microsoft RDS

☐

 Microsoft Virtual Desktop

☐

 AWS Workspaces

☐

Cancel

Save

Paul Pearman

SentryBay Armored Client Portal - Redite

Configure

—

Configure

—

Configure

—

Configure

—



Exclusive Authorised Distributor

REDITE.

Cyber & Data Security



ARMORED CLIENT ADMIN PORTAL



MENU


Dashboard

Home


Companies

Admins


Description




Installed Browsers
Chrome, Firefox, Internet Explorer, Edge, Safari




Microsoft 365
Microsoft Word, Excel, Outlook, PowerPoint




Secure Browser
Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking




Remote Access
Citrix, VMware Horizon, Microsoft RDS, AWS Workspaces



Whitelisted Collaborative Software
TeamViewer, GoToMeeting, RealVNC, Microsoft Teams, Zoom




Registry
Add, Sync and Delete Registry Keys



Custom Settings
Block RDP, Block VM, Protect Clipboard


Whitelisted Collaborative Software


TeamViewer, GoToMeeting, RealVNC, Microsoft Teams, Zoom.



TeamViewer


☐






GoToMeeting


☐






Bomgar


☐






Skype


☐






Snipping Tool


☐






RealVNC


☐






Microsoft Teams


☐





Zoom

☐



Cancel


Save

Custom Settings

Block RDP, Block VM, Protect Clipboard


Block RDP

☐




Block VM

☐



Protect Clipboard


☐



PFX File

No file uploaded.

Add



Cancel

Save

Secure Browser

Allow Settings, Enforce HTTPS, Bookmarks, Certificate Checking

Allow Settings

☐



Allow Printing

☐



Allow Hosts File

☐



Enforce HTTPS

☐



Show Bookmark Bar

☐



Hide App Shortcuts in Bookmark Bar

☐



Bookmarks

Add

The record should be in a name|url format

Certificate Checks

Add

The record should be in a url|certificate name format

URL Whitelist

Add

The record should be a domain

DNS Servers

Add

User Agent

Custom string to be appended to user agent

Homepage URL

The record should be a domain

Paul Pearman

SentryBay Armored Client Portal - Redite

Edit

Configure

-

Configure

-

Configure

-

Configure

-

Configure

-

Configure

-

Configure

-

Exclusive Authorised Distributor

REDITE.

Cyber & Data Security



WHAT ARE THE BENEFITS?

COMPLIANCE

- ISO, NIST, MAS, GDPR, PCI, PSD2, HIPAA, APP's etc.

RISK & PENALTIES REDUCED

- Mitigates financial losses and integrity of brand

COST REDUCTION

- No Corporate 'locked down' hardware required
- Reduction in Cyber-insurance premiums
- Reduced helpdesk support based on previously deployed solutions

SECURE REMOTE ACCESS

- Secure BYOD
- Secure unmanaged devices
- Secure remote access to enterprise for 3rd party vendors / consultants / remote development teams / outsource IT companies etc.

ENFORCEMENT

- Enforce and manage the Armored client on end-user devices. I.e. no remote access unless accessing via Armored Client

EASE OF USE

- Simple, scalable, one time download and install

ENHANCED PRODUCTIVITY

- Empowering employees and 3rd parties to use their own personal devices

CONFIGURABLE PROTECTION

- For multiple application within the Armored client framework

NO INTEGRATION

COMPATIBILITY

- With existing Endpoint Security Software



Exclusive Authorised Distributor

REDITE.
Cyber & Data Security

Confidential: Redite Pty Ltd (Redite). Not To Be Copied, Distributed Or Referred To Without The Prior Written Consent Of REDITE. All Rights Reserved. Proprietary Rights Of REDITE Includes The Following: The REDITE Products, Applications, Manuals, Brochures, Related Data And Information Are The Subject Of Trade Secrets And Copyrights Of REDITE And Are Provided In Confidence. All Use, Disclosure, Copying, Transfer, Reproduction, Display, Distribution, Or Creation Of Derivative Works, Unless Expressly Authorized In The Written License Agreement Between REDITE And The Licensee, Is Strictly Prohibited. Information Is Subject To Change Without Notice And Does Not Represent A Commitment On The Part Of REDITE That The System Performs Every Function And Application. Redite Is The Exclusively Authorised Distributor Of SentryBay

SentryBay

PRODUCT FEATURES & COMPARISON

Features	SentryBay Armored Client	Symantec Fireglass	IBM Trusteer	Comodo Securebox	Bromium
Kernel-level anti-keylogging	✓	✗	✗	✓	✓
Screen capture protection	✓	✗	✓	✗	✓
Screen scraping protection	✓	✗	✗	✗	✓
Protected browser	✓	✓	✗	✓	✓
Locked-down browser	✓	✗	✗	✗	✗
Phishing protection	✓	✓	✓	✗	✓
Protection against malware attacks	✓	✓	Some	✓	✓
DLL injection protection and process hooking protection	✓	✗	✗	✓	✓
Windows, Mac, Linux, mobile platforms	✓	✓	✓	✗	✗
SDK available	✓	✗	✗	✗	✗
Suitable for: <ul style="list-style-type: none">• Managed devices• BYOD• Customers• Suppliers	<div>✓</div> <div>✓</div> <div>✓</div> <div>✓</div>	<div>✓</div> <div>✓</div> <div>✗</div> <div>✗</div>	<div>✗</div> <div>✓</div> <div>✓</div> <div>✓</div>	<div>✓</div> <div>✓</div> <div>?</div> <div>?</div>	<div>✓</div> <div>✗</div> <div>✗</div> <div>✗</div>

Commercial in confidence.
Not to be distributed without
prior written consent from
REDITE.

PRODUCT FEATURES & COMPARISON

	SentryBay Armored Client	Symantec Fireglass	IBM Trusteer	CrowdStrike Falcon	Bromium
Technology type	Anti-key logging, anti-screen capture, anti-code & DLL injection, application containerisation	Web isolation & containerisation through a web proxy	Anti-malware, anti-phishing, anti-key logging	Endpoint threat detection with the engine on the cloud ("EDR" solution)	Process isolation
Sector specialisation	All	All	Retail customers or financial institutions	All	Banking, healthcare, government, manufacturing
Pricing	As per Retail Rates Card	?	Typically 0.50c - \$1.50 per eligible customer p.a. (NB the usage rate is often as low as 10/20% so pricing can look misleading). Pricing likely more similar to SentryBay in enterprise context.	\$110 - \$220 for perpetual license	\$110 - \$220 for perpetual license
Key USPs	Specialist anti-key logging, secure but lightweight containerisation, wide set of use cases, easy to install	Stop malware from reaching the endpoint device	Good traction in retail banking, easy install	Better way of threat detection	Works where detection-based solutions fail

Commercial in confidence.
Not to be distributed without
prior written consent from
REDITE.

PRODUCT FEATURES & COMPARISON

	SentryBay Armored Client	Symantec Fireglass	IBM Trusteer	Crowdstrike Falcon	Bromium
Comment		<p>Tech OK, but quite a narrow solution – just focused on protecting browser activities and prevent virus spread internally, so only partially competing with SB who can protect any remote access, enterprise or SaaS application.</p> <p>Focused on C level employees and high risk browser users – whereas we focus on ALL employees, ALL customers/suppliers/contractors etc.</p> <p>No key-logging protection.</p>	<p>Strong penetration as a retail customer solution for online banking.</p> <p>High level of support issues, issues with their anti-keylogging tech (it is switched off as a default because of this)</p>	<p>Complementary solution which sits alongside ours. Not really a competitor.</p> <p>See section providing a further explanation of the relative pros & cons of EDR solutions and how they compare with SB below.</p>	<p>Heavy solution – heavy to install, heavy on processing and management. Applicable for employees (internal network only), but not easily manageable for remote employees, suppliers or customers.</p> <p>The solution does not provide meaningful security benefits over our solution.</p>

Commercial in confidence.
Not to be distributed without
prior written consent from
REDITE.

OVERVIEW & OPTIONS ARMORED CLIENT



Simple to Deploy and Distribute

- With a package size of less than 50MB, the Armored Client is a lightweight application with minimal administrative requirements
- The software can be deployed from a Redite AWS instance, or hosted within your own infrastructure
- No PC restart is required to implement the software



Configurable Secure Browser

- Based on Chromium Code, with patented SentryBay Core Security Features embedded
- Customise and Control the following browser features:
 - ✓ Site/URL access through a whitelisting facility
 - ✓ Force Certificate Check on certain addresses
 - ✓ Enforce the use of HTTPs on accessed sites
 - ✓ Set and enforce specific homepage addresses
 - ✓ Deploy pre-set browser Bookmarks to users
 - ✓ Show or hide advanced browser features



Optional Credential Monitoring (separate costing)

- Delivers a credential monitoring capability to the enterprise through the Armored Client, or SDK



'Armor' Your Applications

- Using the web based or standalone configuration utility, you can target installed Applications to enable the Core Security Features from the Armored Client
- Specify whether protected Apps run within a secure user container (SAS) or remain within the *logged on* user session



Optional Advanced Malware Detection (separate costing)

Inspect traffic from customer connected devices:

- Examines DNS queries and can check whether generated by a DGA (Domain Generation Algorithm)
- AI engine analyses if the DGA issued request has been generated by malware
- Identify the family of malware
- Alert the SOC, SIEM or customer
- Prevents Sensitive Data leaving the device and being sent to cyber criminals
- 90% Detection Rate with 0.0001% False Positive Rate
- Can be integrated into existing Security Solutions or developed as a separate capability

RETAIL PRICING AND RATES CARD

COMMERCIAL IN CONFIDENTIAL – For Retail Distribution Only.

REGION: AUSTRALIA - Effective 1st October 2020For product information and
sales support please contact

PAUL PEARMAN

New Business Development Manager

Email: paul@redite.co

TIER 1 DESCRIPTION – SENTRYBAY ARMORED CLIENT	PAYMENT REGULARITY	USER BASED LICENSES – ANNUAL SUBSCRIPTION	VOLUME DISCOUNT %	SentryBay Annual RRP (AUD) Ex GST	SentryBay Monthly RRP (AUD) Ex GST
<p>Includes the Armored Client Secure Browser, configurable from the Armored Client Administration portal, plus the protection of Office 365 Apps. This includes Microsoft Word, Excel, Outlook, PowerPoint, Publisher, and OneNote.</p> <p>The Armored Client secure browser will also offer a protected means for accessing Microsoft Office 365 Web Apps, such as SharePoint Online and Yammer, and the browser versions of the Office Suite.</p> <p>Non-Microsoft SaaS based apps can be configured through the secure browser, protecting sensitive data from endpoint threats.</p>	Annual or Monthly	10 – 499	0%	\$92.00	\$7.67
	Annual or Monthly	500 – 999	On Request	On Request	On Request
	Annual or Monthly	1000 - 1999	On Request	On Request	On Request
	Annual In Advance	2000 - 2999	On Request	On Request	On Request
	Annual In Advance	3000 - 4999	On Request	On Request	On Request
	Annual In Advance	5000 +	On Request	On Request	On Request
TIER 2 DESCRIPTION – SENTRYBAY ARMORED CLIENT	PAYMENT REGULARITY	USER BASED LICENSES – ANNUAL SUBSCRIPTION	VOLUME DISCOUNT %	SentryBay Annual RRP (AUD) Ex GST	SentryBay Monthly RRP (AUD) Ex GST
<p>Includes all features from Tier 1, as well as protecting any Remote Access solution such as Citrix, VMware Horizon, Windows Virtual Desktop, Amazon Workspaces or legacy RDS environments.</p> <p>The Armored Client will protect client software installed on the endpoint.</p> <p>Note – This per user cost excludes any remote access services currently in use by the organization.</p>	Annual or Monthly	10 – 499	0%	\$138.00	\$11.50
	Annual or Monthly	500 – 999	On Request	On Request	On Request
	Annual or Monthly	1000 - 1999	On Request	On Request	On Request
	Annual In Advance	2000 - 2999	On Request	On Request	On Request
	Annual In Advance	3000 - 4999	On Request	On Request	On Request
	Annual In Advance	5000 +	On Request	On Request	On Request

Exclusive Authorised Distributor

REDITE.
Cyber & Data Security

*Pricing based in AUD\$, GST Sales Taxes Apply, Exchange Rate subject to fluctuation and revision. Excludes localisation, hosting and implementation cost, additional ad hoc software development specific to the client is billed on a time and cost basis. Minimum order quantity apply, 12 Month warranty Included. Refer to product feature list and presentation for detailed and complete feature list. Conditions Apply, Product features are subject to change. The right to introduce modifications is reserved.



YOUR SECURITY REDEFINED

COMPUTER TROUBLESHOOTERS Net Revenue Share

COMMERCIAL IN CONFIDENTIAL.

REGION: AUSTRALIA - Effective 1st October 2020

Reseller – Net Revenue share Rebate

Type	Sign On – Initial 12-month Term allocation	Annual – 12-month Terms Renewals allocation
Spotter (Refer directly to Redite)	2%	0%
Direct Customer (Managed Support)	10%	5%

Special Incentive for Computer Troubleshooters Franchisee

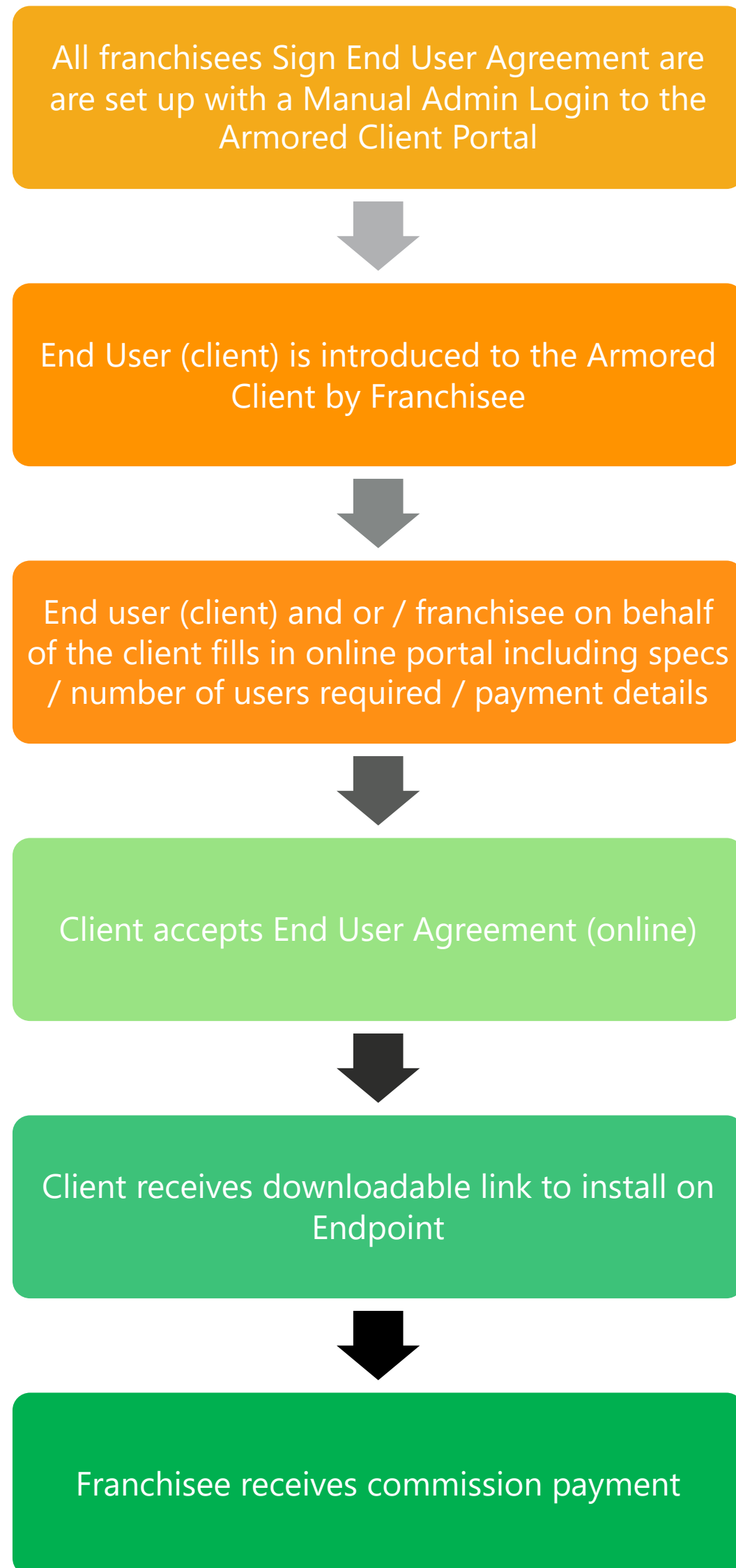
For every 500 new users in an annualized year the franchisee will receive a special one-off incentive payment	
Payment to Franchisee	\$2,000 ⁺⁺

⁺⁺ Target of 500 new users is per Franchisee. Payment of Incentive is paid quarterly.

YOUR SECURITY REDEFINED

CUSTOMER PROCESS

Customer Portal
www.redite.co



SERVICE AND SUPPORT

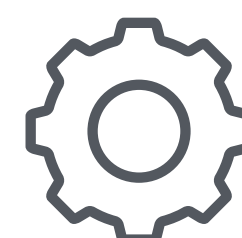


SOFTWARE AS A SERVICE

Fully managed service, we take care of the complexity and you enjoy the protection.

-

Billing monthly or yearly, we have volume price structure from 500 users up to 30 000 users.



CONFIGURED TO YOUR NEEDS

The Armored Product comes with a range of configuration which your IT team can configure to optimize the deployment and create a rollout strategy

-

We work with your team to structure the smooth deployment with optimal protection.



PASSIONATE SUPPORT

We are able to back up your current first line support team with our experts, for escalated support issues.

-

Alternatively, we are able to offer a first line support team to handle support requests from the end point.

SALES & SUPPORT DETAILS

REDITE Support Logging Services and Procedures

All support requests can be e-mailed 24/7 directly with supporting documents through to support@redite.co.

On receipt of your email, your support request will be logged by the support desk into the Support system and you will receive a support ticket confirming your request. Please quote the support ticket number with all correspondence.

Once your request has been completed you will receive a closure notification confirming that your support request has been actioned and that your support ticket has now been closed.

Alternatively, during the hours 09h00 – 16h00, a phone call can be placed directly to the support desk 1300 010 733. The support desk will book any support request directly into our Support System and generate the support ticket and manage the call process.

Platform Configuration Service requests - Programming and system enhancements requests can be scheduled for discussion directly with our program management team via an online WebEx meeting. These meetings and any project support requests and proposals will be billed out to clients at \$ 155.00 (Ex GST) per hour or any part thereof. These requests can be emailed through to support@redite.co.

Account Queries – These services are outsourced; all accounting service queries can be logged through REDITE Support or directly with accounts@redite.co.

Call Priority	Monday – Friday 08h30 – 16h00 Support Desk Response Time	Support Desk Resolution Time	Deployment Services
High 1	90 Minutes	10 hours	Or Per Project Plan
Medium 2	90 Minutes	7 Days	Or Per Project Plan
Project 3	72 Hours	Per project Estimate	Or Per Project Plan
Outside of Contracted Support	Billable at \$155.00 per hour		
System Down / After Hours Business Critical	120 Minutes / Billable at \$155 per hour	As Practical – Task & Developer Dependent	Per Project Plan

Any Support desk requests not actioned within the resolution times can be tabled directly with calvinh@redite.co.

System Down / After Hours Business Critical Support – SMS fault with contact details to;
+61 434378600/ +61 434378602. Support phone calls received will be billed at \$250.00 per hour if not on pre-purchase support plan.

Support Desk business Hours: Monday to Friday 08h30 – 16h00, Contact 0434378600.

National Sales Contact: Paul Pearman, Redite New Business Development Manager, Contact Phone 0429 877 623 Contact Email paul@redite.co

SALES COLLATERAL OVERVIEW

All sales Collateral can be downloaded from
<https://redite.co/reseller>

Collateral Pack consists of

1 x Armored Client Double Sided Flyer	(PDF)
1 x Armored Browser Double Sided Flyer	(PDF)
1 X Armored Client Powerpoint Presentation	(Powerpoint & PDF)
1 x Administration Portal Guide	(PDF)
1 x Armored Client Installation Guide	(PDF)
1 x VDI Access White Paper for Armored Client	(PDF)
1 x SentryBay Usage Cases Document	(PDF)
1 x Redite Reseller Sales & Support Guide (This Document)	(PDF)
All Redite / SentryBay / Armored Client Logos	(JPEG, AI FILES)
1 x Updated Press Kit	(Document with live links)
Armored Client for MAC Demo	(MP4)
Armored Client for Windows	(MP4)
Armored Client protecting local Office Word	(MP4)
Armored Client WebPortal Configuration	(MP4)
Armored Client Secure Browser	(MP4)
Armored Client for Citrix	(MP4)
Podcast Channel Daily News Sentrybay	(MP3)

Documents relating to architecture of specific products available on request and on the receipt of a Mutual Non Disclosure Agreement being signed by the Reseller (FRANCHISEE) and the Distributor (REDITE).

Exclusive Authorised Distributor



REDITE.

Cyber & Data Security

AUTHORISED
DISTRIBUTOR



PAUL PEARMAN

New Business Development Manager

Email: paul@redite.co

Mobile: +61 429 877 623